REMARKS

Claims 1, 4-22 were rejected under 35 U.S.C. 103(a) as being unpatentable over High-bandwidth Digital Content Protection System, Revision 1.0 by Intel Corporation (HDCP Revision 1) in view of U.S. Patent 5,142,578 issued to Matyas et al.

The Applicants would like to thank the Examiner for the timely response. However, upon thorough consideration of both references, the Applicants respectfully disagree with the Examiner's obviousness type rejection for at least the following reasons. In both references, there is but a single encryption protocol used to encrypt the cryptographic keys. This is evident in the HDCP reference starting on page 6,first paragraph describing the authentication protocol and more particularly, in section 2.1 Overview, "Each authorized participant...receives an array of 40, 56 bit secret device keys and a corresponding identifier from the Digital Content Protection LLC. This identifier is the Key Selection Vector (KSV) assigned to the device. **The KSV is a 40 bit binary value**." (emphasis added) Therefore, the HDCP authentication protocol relies upon a single encryption/decryption protocol (described in detail in section 2.2) that uses the single 40 bit binary KSV that is assigned to the device.

Furthermore, the Matyas reference merely describes a method of distributing a hybrid public key algorithm/data encryption algorithm key using control vectors. More particularly, Matyas describes a method and apparatus for securely distributing an initial Data Encryption Algorithm (DEA) key-encrypting key by encrypting a key record (consisting of the key-encrypting key and control information associated with that key-encrypting key) using a public key algorithm and a public key belonging to the intended recipient of the key record (at Abstract). In this way, Matyas merely assures that the proper recipient has received the appropriate key and does not teach nor remotely suggest that the keys themselves are encrypted/decrypted based upon a selected one of a plurality of available encryption/decryption protocols. For example, Matyas " describes a method and apparatus to improve the integrity of the key distribution process by applying a digital signature to the key record and by including

identifying information (i.e., an originator identifier) in the control information of the key record" (at Abstract).

Unfortunately, even by if the proper key recipient is assured by the system described by Matyas (as it is already provided by the HDCP system), by relying upon a single encryption/decryption protocol, the HDCP system is susceptible to "hacking" if that single encryption/decryption protocol is compromised. This general shortcoming of the prior art is described in the specification at page 12, first full paragraph:

> One problem with the above embodiment is that an unauthorized third party may retrieve the encrypted key multiple times and attempt to decipher the unencrypted key. To discourage such attempts, support for multiple encryption/decryption protocols (for encrypting the keys) may be provided within integrated circuit 201, and the keys may be encrypted according to one of the protocols. The OEM may specify the specific protocol by using appropriate commands. The data indicating the specific protocol may also be stored thereafter in serial EEPROM 250 to facilitate later decryption by HDCP engine 290.

Therefore, the invention solves this problem by providing for a selection of one of a number of available encryption/decryption protocols **to encrypt the keys** the selection of which is unknown to any outside agent. In particular, claim 1 recites:

> "A method of using a number of a plurality of cryptographic keys in a display device having a printed circuit board (PCB) and a master block, comprising:
>
> providing the number of the plurality of keys to the PCB by the master block;
>
> selecting one of a number of available encryption protocols for each of the provided keys;
>
> encrypting each of the provided keys based upon a particular one of the selected encryption protocols".

In this way, the invention provides an additional layer of security since each key may in fact have been encrypted by a separate and different encryption protocol known only to the master block therefore preventing the shortcoming of encrypting all the cryptographic keys with the same encryption protocol as is done with both the HDCP and Matyas references.

Therefore, the Applicants believe that neither of the cited references taken singly or in any combination render the invention as recited in claim 1 unpatentable and respectfully request that the Examiner withdraw the U.S.C. 103(a) rejection of claim 1 and all claims dependent thereon.

Independent claim 12 recites the same limitation as does claim 1 and therefore the Applicants also believe that claim 12 and all claims dependent thereon are allowable for at least the same reasons stated above for claim 1.

CONCLUSION

In view of the foregoing, it is respectfully submitted that all pending claims are allowable. Should the Examiner believe that a further telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,

BEYER WEAVER & THOMAS, LLP

Michael J. Ferrazano
Reg. No. 44,105

P.O. Box 70250
Oakland, CA 94612-0250
(650) 961-8300